PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-056681
(43)Date of publication of application : 25.02.2000

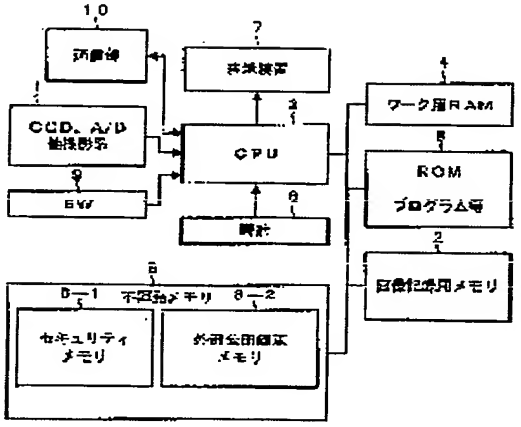
(51)Int.Cl. G09C 1/00
G06F 12/14
G09C 5/00
H04N 1/44

(21)Application number : 10-236342
(22)Date of filing : 07.08.1998

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : IIZUKA NORIO

(54) DIGITAL DATA RECORDER WITH SECURITY INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a digital data recorder with secrity information which prevents digital data from being falsified, reproduced, partially used, or illegally used.
SOLUTION: A CPU 3 generates a public key and a secret key by a public key cryptosystem. Then, an ID image stored in a security memory 8-1 is used as a random number series source. Moreover, the CPU 3 appends additional information to the image data inputted from a pickup system 1, and encodes the data with the secret key, to generate an electronic signature data. Further, the CPU summarizes the input data main body to which the additional information is appended, the electronic signature data, and the public key, etc., an generates a data file. In the case of restoring the data file, if the data acquired by decoding the electronic signature data by using the public key appended to the data file coincides with the data acquired from the main body of the data file, it can be judged that neither falsification nor edit, etc., are added thereto.



LEGAL STATUS

[Date of request for examination]	14.04.2003
[Date of sending the examiner's decision of rejection]	05.09.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2005-18953
[Date of requesting appeal against examiner's decision of rejection]	30.09.2005
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－56681
（P2000－56681A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	５Ｂ０１７
	６４０		６４０Ｂ	５Ｃ０７５
	６６０		６６０Ｄ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ	
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		

審査請求　未請求　請求項の数16　ＦＤ　（全 17 頁）　最終頁に続く

(21)出願番号　特願平10－236342

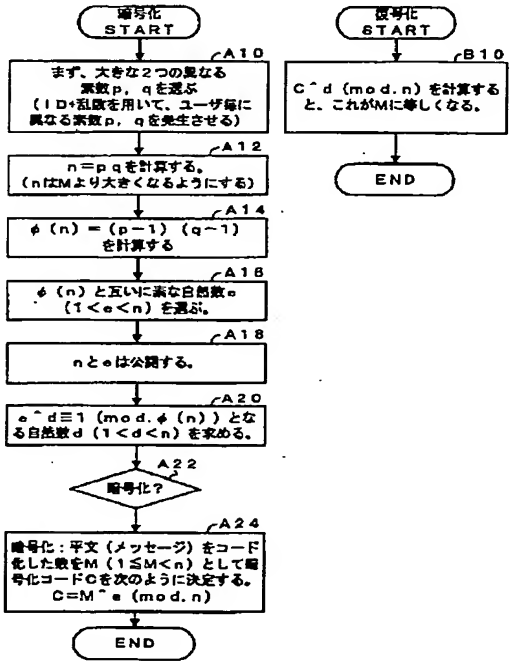
(22)出願日　平成10年８月７日(1998.8.7)

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　飯塚　宜男
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(74)代理人　100096699
弁理士　鹿嶋　英實

Ｆターム(参考)　5B017 AA06 AA07 BA05 BA07 BA09
BB02 BB07 CA12 CA16
5C075 CA14 CD05 CD07 EE02 EE03
FF90

(54)【発明の名称】　セキュリティ情報付きデジタルデータ記録装置

(57)【要約】
【課題】　デジタルデータの改竄や複製、部分使用、不正使用を防止できるセキュリティ情報付きデジタルデータ記録装置を提供する。
【解決手段】　ＣＰＵ３は、公開鍵暗号方式により公開鍵および秘密鍵を生成する。このとき、セキュリティメモリ８－１に格納されているＩＤ画像を乱数系列発生源として用いる。また、ＣＰＵ３は、撮影系１から入力された画像データに付加情報を添付し、該データを上記秘密鍵により暗号化し、電子署名データを生成する。さらに、上記付加情報が添付された入力データ本体、電子署名データ、上記公開鍵等をまとめ、データファイルを生成する。該データファイルを復元する際には、データファイルに添付されている公開鍵を用いて電子署名データを復号化して取得したデータと、データファイルのデータ本体から取得したデータとが一致すれば、改竄、編集等が加えられていないと判断できる。



1

【特許請求の範囲】

【請求項１】　公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、　デジタルデータを入力する入力手段と、

前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、

前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、

前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、

前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【請求項２】　前記閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化する復号化手段と、

前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断する判断手段と　前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示する表示手段とを具備することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項３】　前記入力データ本体が暗号化される前段で、入力データ本体から特徴データを抽出し、ダイジェスト化する特徴データ抽出手段を具備し、

前記電子署名手段は、前記特徴データ抽出手段によりダイジェスト化されたデータを、前記鍵生成手段により生成された秘密鍵により暗号化し、電子署名データを生成することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項４】　前記鍵生成手段は、デジタルデータの記録者を識別するための識別データに基づいて、公開鍵および秘密鍵を生成することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項５】　前記識別データは、デジタルデータの記録者が選択した任意の識別画像データであることを特徴とする請求項４記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項６】　前記識別画像データを所定のサイズに間引く間引き手段を具備し、

前記付加情報生成手段は、前記間引き手段により間引かれた識別画像データを前記入力手段から入力されたデジタルデータに付加情報として添付することを特徴とする請求項５記載のセキュリティ情報付きデジタルデータ記録装置。

2

【請求項７】　配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データを記憶する配信相手情報記憶手段と、

前記配信相手情報記憶手段に記憶されている識別画像データを指定することで、前記閲覧ファイル生成手段により生成された閲覧ファイルの配信相手を選択する配信先選択手段とを具備することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項８】　配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、

前記電子署名生成手段により生成された電子署名データを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段を具備し、

前記閲覧ファイル生成手段は、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生成することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項９】　前記公開情報は、少なくとも、公開可能な画像データを含むことを特徴とする請求項８記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１０】　前記閲覧ファイルを自身の秘密鍵により復号化する第２の復号化手段と、

前記復号化手段は、前記第２の復号化手段により復元されたデータに添付されている公開鍵により、復元されたデータに添付されている電子署名データを復号化することを特徴とする請求項９記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１１】　前記判断手段は、前記第２の復号化手段による復元が失敗した場合には、前記閲覧ファイルが不正に入手されたと判断し、

前記表示手段は、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示することを特徴とする請求項１０記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１２】　前記公開情報は、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであるかを示すファイル種別情報を含むことを特徴とする請求項１ないし１１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１３】　前記電子署名手段による電子署名データの生成に先立って、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段を具備

することを特徴とする請求項１記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１４】　前記判断手段は、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断することを特徴とする請求項１３記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項１５】　公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、

デジタルデータを入力する入力手段と、

前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、

前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、

配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、

前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、

前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する第１の閲覧ファイル生成手段と、

前記第１の閲覧ファイル生成手段により生成された閲覧ファイルを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段と、

ファイル本体の種別を示すファイル種別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データをまとめ、特定の相手に対する閲覧ファイルを生成する第２の閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【請求項１６】　公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、

デジタルデータを入力する入力手段と、

前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段と、

前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記電子透かし手段により電子透かしが施されたデータに添付する付加情報生成手段と、

前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、

前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、

前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子スチルカメラ等のデジタルデータ記録装置に係り、記録したデジタルデータの閲覧・配信に際し、セキュリティ向上を図るセキュリティ情報付きデジタルデータ記録装置に関する。

【０００２】

【従来の技術】電子スチルカメラ等の入力／デジタル変換機器は、パソコンとの装置との接続・転送のしやすさから、著作物的な意味合いや、業務上の記録、証拠などに用いることができるが、デジタルデータであるがゆえに、編集、改竄を比較的自由に行うことができる。

【０００３】一方、通信や当事者間の通信のセキュリティのためには、当事者間の秘密通信や、内容証明通信のために、公開鍵方式や、共有鍵方式を応用した暗号化および電子署名の主々の方式や、不正複製や一部流用の検出／抑止のため、特に著作権情報等を入れ込むための、電子透かしなどの処理がある。

【０００４】これら既存の方式により、パソコンに取り込んだ画像や音声、動画データに対して、セキュリティに対する対策を施すことは可能である。しかし、これらは、パソコン上の処理プログラムになっており、生データである画像や音声のファイルの記録／生成時については、保証する方法がなかった。

【０００５】

【発明が解決しようとする課題】したがって、デジタル画像データ等の生データファイルについては、当事者間の秘密通信においても、また、インターネットのＷｅｂ公開等で、デジタル署名を付加して内容保証をしたデータであろうと、電子スチルカメラ＞ＰＣの経路において、および、撮影した瞬間の、保証ができていないため、不正入手した画像をパソコンに取り込んだ時点で、保証データを付加した否かは判定することができなかった。

【０００６】また、業務において、デジタル画像等を用いる場合にも、改竄を防止するなど、データの正当性が証明されいなくてはならず、これは、生データ撮影時（作成時）に付加されるのでなければ、セキュリティ的にもユーザの使い勝手としても、問題であった。また、電子透かしにおいても、撮影した画像がそのまま著作物として利用されることを考えると、データの作成時に情報を入れ込めないので、同様の問題があった。

【０００７】そこで本発明は、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるセキュリティ情報付きデジタルデータ記録装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的達成のため、請求項１記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とする。

【０００９】また、好ましい態様として、例えば請求項２記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、前記閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化する復号化手段と、前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断する判断手段と前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示する表示手段とを具備することを特徴とする。

【００１０】また、好ましい態様として、例えば請求項３記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、前記入力データ本体が暗号化される前段で、入力データ本体から特徴データを抽出し、ダイジェスト化する特徴データ抽出手段を具備し、前記電子署名手段は、前記特徴データ抽出手段によりダイジェスト化されたデータを、前記鍵生成手段により生成された秘密鍵により暗号化し、電子署名データを生成することを特徴とする。

【００１１】また、好ましい態様として、例えば請求項４記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、前記鍵生成手段は、デジタルデータの記録者を識別するための識別データに基づいて、公開鍵および秘密鍵を生成することを特徴とする。

【００１２】また、好ましい態様として、例えば請求項５記載のように、請求項４記載のセキュリティ情報付きデジタルデータ記録装置において、前記識別データは、デジタルデータの記録者が選択した任意の識別画像データであることを特徴とする。

【００１３】また、好ましい態様として、例えば請求項６記載のように、請求項５記載のセキュリティ情報付きデジタルデータ記録装置において、前記識別画像データを所定のサイズに間引く間引き手段を具備し、前記付加情報生成手段は、前記間引き手段により間引かれた識別画像データを前記入力手段から入力されたデジタルデータに付加情報として添付することを特徴とする。

【００１４】また、好ましい態様として、例えば請求項７記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データを記憶する配信相手情報記憶手段と、前記配信相手情報記憶手段に記憶されている識別画像データを指定することで、前記閲覧ファイル生成手段により生成された閲覧ファイルの配信相手を選択する配信先選択手段とを具備することを特徴とする。

【００１５】また、好ましい態様として、例えば請求項８記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、前記電子署名生成手段により生成された電子署名データを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段を具備し、前記閲覧ファイル生成手段は、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生成することを特徴とする。

【００１６】また、好ましい態様として、例えば請求項９記載のように、請求項８記載のセキュリティ情報付きデジタルデータ記録装置において、前記公開情報は、少なくとも、公開可能な画像データを含むことを特徴とする。

【００１７】また、好ましい態様として、例えば請求項１０記載のように、請求項９記載のセキュリティ情報付きデジタルデータ記録装置において、前記閲覧ファイルを自身の秘密鍵により復号化する第２の復号化手段と、前記復号化手段は、前記第２の復号化手段により復元されたデータに添付されている公開鍵により、復元されたデータに添付されている電子署名データを復号化することを特徴とする。

【００１８】また、好ましい態様として、例えば請求項１１記載のように、請求項１０記載のセキュリティ情報付きデジタルデータ記録装置において、前記判断手段は、前記第２の復号化手段による復元が失敗した場合に

は、前記閲覧ファイルが不正に入手されたと判断し、前記表示手段は、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示することを特徴とする。

【００１９】また、好ましい態様として、例えば請求項１２記載のように、請求項１ないし１１記載のセキュリティ情報付きデジタルデータ記録装置において、前記公開情報は、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであるかを示すファイル種別情報を含むことを特徴とする。

【００２０】また、好ましい態様として、例えば請求項１３記載のように、請求項１記載のセキュリティ情報付きデジタルデータ記録装置において、前記電子署名手段による電子署名データの生成に先立って、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段を具備することを特徴とする。

【００２１】また、好ましい態様として、例えば請求項１４記載のように、請求項１３記載のセキュリティ情報付きデジタルデータ記録装置において、前記判断手段は、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断することを特徴とする。

【００２２】また、上記目的達成のため、請求項１５記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する第１の閲覧ファイル生成手段と、前記第１の閲覧ファイル生成手段により生成された閲覧ファイルを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段と、ファイル本体の種別を示すファイル種別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データをまとめ、特定の相手に対する閲覧ファイルを生成する第２の閲覧ファイル生成手段とを具備することを特徴とする。

【００２３】また、上記目的達成のため、請求項１６記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記電子透かし手段により電子透かしが施されたデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段と具備することを特徴とする。

【００２４】

【発明の実施の形態】まず、実施例に先立ち、本実施例が前提とする公開鍵暗号方式のうち、ＲＳＡ公開鍵暗号方式について簡単に説明しておく。ＲＳＡ公開鍵暗号とは、１９７９年に，ＭＩＴ（マサチューセッツ工科大学）のＲｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｅｌｍａｎが提唱した方式である。なお、ＲＳＡ公開鍵暗号については、米国特許４，４０５，８２９号（暗号通信システムと手法）などで述べられている。

【００２５】なお、本実施例では、特にＲＳＡ暗号でなくとも、公開鍵方式で、暗号化とデジタル署名の両方を行うことのできる暗号化方式なら暗号化方式には制限はない。また、暗号化ファイルのやりとりの機能に関してだけなら、本実施例とほとんど同じ態様で、共通鍵方式の暗号（ＤＥＳ、ＦＥＡＬなど）にも対応可能である。ここで、図１は、ＲＳＡ公開鍵暗号方式を説明するためのフローチャートである。以下、図１のフローチャートを参照してＲＳＡ公開鍵暗号方式を説明する。

【００２６】まず、暗号化処理においては、ステップＡ１０で、大きな２つの異なる素数ｐ、ｑを選ぶ。本実施例では、ユーザ毎に特有のＩＤと乱数とを用いて、ユーザ毎に異なる素数ｐ、ｑを生成している。次に、ステップＡ１２で、ｎ＝ｐｑを計算する。このとき、ｎは、後述するＭより大きくなるようにする。次に、ステップＡ１４で、ϕ（ｎ）＝（ｐ－１）（ｑ－１）を計算し、ステップＡ１６で、ϕ（ｎ）と互いに素な自然数ｅ（１＜

ｅ＜ｎ）を選び、ステップＡ１８で、上記ｎとｅとを公開する。

【００２７】次に、ステップＡ２０で、ｅ＾ｄ≡１（ｍｏｄ．φ（ｎ））となる自然数ｄ（１＜ｄ＜）を求める。上記（ｎ，ｅ）のペアが公開鍵、ｄが秘密鍵となる。また、素数ｐ、ｑは秘密であり、絶対公開してはならない値である。公開鍵（ｎ，ｅ）から秘密鍵ｄを求めることは困難であることが知られている。そして、ステップＳ２２で、暗号化か否かを判断し、暗号化であれば、ステップＡ２４で、平文（メッセージ）をコード化した数をＭ（１≦Ｍ＜ｎ）として、公開鍵（ｅ，ｍ）を用いて、Ｃ＝Ｍ＾ｅ（ｍｏｄ．ｎ）なる演算で暗号コードＣを生成する。

【００２８】また、復号化処理では、ステップＢ１０で、暗号化されたコードＣ、秘密鍵ｄ、ｅとｄの関係により決まる係数ｎに従って、Ｍ＝Ｃ＾ｄ（ｍｏｄ．ｎ）を計算することで、元のッセージＭを取得する。秘密鍵ｄは、受信した相手のみが知っているので、該受信者しか復号化できないようになっている。

【００２９】なお、本実施携帯による公開鍵を用いた暗号化手法には、以下の特徴がある。

［公開鍵暗号について］

１．暗号化鍵と復号化鍵を別のものにする。

２．暗号化は極めて容易である。

３．鍵なしで復号化することは，たとえ仕組みがわかったとしても，事実上不可能である。

４．暗号化鍵は公開する（公開鍵）。復号化鍵は秘密（秘密鍵）とする。

５．秘密鍵で暗号化したデータを本文に付加し、公開鍵で確認させることで、本文データを公開したまま、改竄やなりすましを防止する、デジタル署名が可能である（但し、全ての公開鍵がデジタル署名には対応していない）。

【００３０】Ｂ．第１の実施形態

以下、本発明の実施形態を、電子スチルカメラに適用した一実施例として、図面を参照して説明する。

【００３１】図２は、本発明の第１の実施の態様における電子スチルカメラの構成を示すブロック図である。図において、撮影系１は、レンズを介して結像した静止映像を電気信号に変換するＣＣＤ、上記静止映像信号をデジタルデータ（以下、画像データという）に変換するＡ／Ｄ変換器等からなり、画像データをＣＰＵへ供給する。画像記録用メモリ２は、図示しない圧縮／伸張手段により、例えばＪＰＥＧ（Joint Photographic Coding Experts Group）方式などの圧縮方式により圧縮された、画像データ（輝度信号と色信号）を格納する。画像記録用メモリ２は、交換可能な、フラッシュメモリカードなどのメディアになっている場合もある。

【００３２】ＣＰＵ３は、プログラムを実行することにより、電子スチルカメラ全体の動作を制御する。ＲＯＭ５には、ＣＰＵ３で実行される上記プログラムが格納されている。ワーク用ＲＡＭ４は、ＣＰＵ３のワーキングエリアとして用いられる。計時部６は、クロックをカウントすることにより日時を計時し、ＣＰＵ３に供給する。表示装置７は、液晶表示器からなり、撮影系により撮影した映像や（リアルタイム表示）、画像記録用メモリ２に格納した撮影後の画像データを表示する。

【００３３】不揮発メモリ８には、本発明の重要な構成要素を含む情報が格納される。これは、上述したように、画像記録用メモリ２が交換可能になっている場合には、本構成図のように、別ブロックとなっていることが必要である。このセキュリティ処理に関係する不揮発メモリ８は、その機器自体に関するセキュリティ情報を保存するセキュリティメモリ８－１と、外部のユーザの公開鍵を管理する公開鍵束メモリ８－２とに分かれる。

【００３４】セキュリティメモリ８－１には、図３（ａ）に示すように、自身の機器固有ＩＤ、ＩＤ画像、機器使用に必要とされるパスワード情報、暗号化する際に用いる暗号化秘密鍵データ、および公開鍵データが格納されている。機器固有ＩＤは、あらかじめ製造時に書き込まれるユニークな値であり、ランダムな値や製造番号等である。ＩＤ画像は、ユーザ間のファイル転送／通信において、送信元ユーザを受信ユーザに認識させるために、転送される画像データに添付される。

【００３５】ＩＤ画像としては、画像で示されるＩＤとし、例えば、ユーザの顔や、好きなイラスト、趣味に関わる静物などの画像を用いる。ＩＤ画像の格納形態としては、転送やメモリ容量の負担の軽減のため、１６×１６や、３２×３２などの小さな画像（サムネイル）に変換して取り扱う。サムネイルに変換するため、元の情報が失われるので、乱数系列の元をたどれないと言う意味でも、サムネイル変換は効果がある。パスワード情報は、セキュリティにかかわる操作や、カメラ操作全体に対して、ユーザ認証を行うためのものである。該セキュリティメモリ８－１のデータは、ユーザが初めてこの機器を所有した場合に記録され、以後は、基本的には書き換えられない。

【００３６】公開鍵束メモリ８－２は、図３（ｂ）に示すように、画像データを暗号化して送信する相手毎に、その相手にのみ暗号化された画像データを復元できるようにするために、画像データを暗号化する際に用いる公開鍵、ＩＤ画像、および相手の機器を特定するための機器ＩＤを格納している。該ＩＤ画像は、ユーザ間のファイル転送／通信において、データを送信する際に受信ユーザを選択するために用いられる。これら公開鍵束メモリ８－２の情報は、随時追加更新される。

【００３７】また、撮影時の保証データを唯一無二とするために、秘密鍵や、パスワードは、転送不可となっており、メモリ上の格納形式でも、プログラムと組み合わせての暗号化を行い、ハードウェアの分解などによる、

悪意ある情報奪取に対しても強くしてあることが望ましい。

【００３８】スイッチ部９は、シャッタースイッチ、表示画像送りスイッチ、カーソルキー等から構成され、各スイッチのオン／オフ状態はＣＰＵ３により検出される。通信部１０は、パソコン等に画像データを転送するインターフェースや、外部機器へ画像データを通信回線を介して送信するモデムなどの通信手段である。

【００３９】Ｃ．第１の実施形態の動作

以下、全体動作を図４ないし図６に示すフローチャートを参照して説明する。

Ｃ－１．セキュリティ情報生成処理

機器に電源が投入されると、まず、ステップＳ１０で、初期化が行われ、ステップＳ１２で、セキュリティメモリ８－１の内容を確認し、ステップＳ１４で、初回起動であるか否かを判断する。初回起動である場合には、機器の使用に先立って、ユーザが、ユーザ独自のセキュリティ情報を生成しなくてはならない。前述したように、ＲＳＡ暗号系を生成するためには、ＩＤ、秘密鍵ｄ、公開鍵ｅ、およびそれらの管理のためのパスワードを生成する必要がある。ＩＤについては、本実施例では、機器固有ＩＤおよびユーザＩＤ（ＩＤ画像）の２つを組み合わせたものを用いる。

【００４０】このように２つのＩＤ情報を組み合わせる目的は、機器固有ＩＤを暗号化するなどの管理を行うことで、たとえ、この発明に関わる全ての処理方法が悪用されて、カメラレベルからの偽造が行われた場合も、機器固有ＩＤに、正当な値であるかの検出を行うというもう１段階のセキュリティを加えられることと、ユーザＩＤも加えたのは、ユーザ間のファイル転送／通信において、転送された画像データの送信元ユーザが受信ユーザに容易に認識できるという利点のためである。

【００４１】機器固有ＩＤは、前述したように、図２に示すセキュリティメモリ８－１に製造時に、あらかじめユニークな値として書き込まれている。さらに、ユーザがユーザＩＤを生成する。本実施例では、ユーザＩＤとしてユーザが予め設定した画像（ＩＤ画像：サムネイル、１６×１６）を用いている。これにより、キー操作による文字列入力を少しでも省くことができ、文字列よりも見た目にわかりやすいＩＤとなる。

【００４２】そして、図４に示すステップＳ１４で、初回起動であると判別されると、まず、ＩＤ画像の撮影要求モードになる。ステップＳ１６で、ＩＤ画像（例えば、ユーザの顔や、好きなイラスト、趣味に関わる静物など）を撮影し、所定の圧縮方式により圧縮し、例えば１６×１６ドットのサムネイル画像とする。

【００４３】次に、ステップＳ１８で、ユーザにパスワードを要求する。このパスワードは、セキュリティにかかわる操作や、カメラ操作全体に対して、ユーザ認証を行うためのものである。パスワードに関しては、機器使用に際して繰り返し入力される必要があるため、ＩＤのように画像入力を使えないので、キーを用いた英数字入力等を必要とする。但し、機器レベルのセキュリティ不要とユーザが判断した場合は、このパスワード設定処理を省略することができる。

【００４４】次に、ステップＳ２０で、以下の手順に従って秘密鍵ｅ、公開鍵ｄを生成する。まず、図１に示すステップＡ１０に従い、大きな２つの異なる素数ｐ，ｑを選ぶ処理を行う。このために、

ｆ（機器ＩＤ、画像ＩＤ）＝（ｐ，ｑ）

なる関数ｆを処理することにより、鍵発生を行う。

【００４５】この鍵発生アルゴリズムにおいては、比較的大きな素数の組み合わせを、異なるユーザ間で絶対重ならないように設定する必要があり、入力データに乱数発生機構を用いた素数発生処理を行うのが通常である。数式による疑似乱数発生から素数発生の方法だと、アルゴリズムが明らかになると、同じキーの偽造生成が行い易いので、実際のパソコン上の暗号ソフトウェア等では、キー入力間隔やマウスの座標等々を用いて、ランダム系列の発生源としている。本実施例では、同様に決定論的な課程に従わない乱数系列源として、ＩＤ画像そのものを、ランダム系列の発生源としている。

【００４６】なお、ＩＤ画像は、輝度データそのままでは、撮影条件、撮影対象により、値にばらつきがあるので、後述のハッシュ関数をかけるなどして、データブロックごとの値のばらつきを一様に行うなどの処理が必要である。ｐ，ｑが求まれば、図１のステップＡ１２以降に述べた手順に従って、公開鍵ｅ、秘密鍵ｄを生成する。

【００４７】そして、ステップＳ２２で、ＩＤ画像をサムネイル化し、セキュリティメモリ８－１に格納し、ステップＳ２４で、パスワード情報、公開鍵ｅ、秘密鍵ｄをセキュリティメモリ８－１に格納する。

【００４８】Ｃ－２．撮影データ保証情報付加処理

次に、通常の撮影でデジタル署名が付加され、撮影時点でデータ内容が保証されたファイルが生成される動作に付いて説明する。

【００４９】機器に電源が投入された際に、初回起動でない場合には、ステップＳ１４から図５に示すステップＳ２６へ進む。ステップＳ２６では、機器の動作モードがＲＥＣ（撮影）モード、ＰＬＡＹ（再生）モード、通信モードのいずれであるかを判断する。ここで、ＲＥＣモードに設定されている、またはＲＥＣモードが選択された場合には、ステップＳ２８で、撮影処理を行い、ステップＳ３０で、デジタル署名付加を行った後、画像記録用メモリ２に格納し、ステップＳ２６へ戻る。

【００５０】ここで、図７に、ソースとなる画像や日時等の情報をどのようにして、デジタル署名付のデータファイルとするかを模式的に表している。図示するように、撮影データ本体は、撮影時の日時情報、セキュリテ

ィメモリ８－１に格納されている機器ＩＤ、撮影者ＩＤ（ＩＤ画像）および圧縮済みの画像データからなる。なお、画像データは、撮影時に圧縮されるが、これに限らず、暗号化後に全体を圧縮するようにしてもよい。まず、上記撮影データ本体からハッシュ関数で特徴データを抽出し、次いで、該ダイジェスト化されたデータに対し、秘密鍵で暗号化を施し、電子署名データを生成する。そして、ヘッダ（識別、領域情報等）・ファイルタイプ（内容証明）、公開鍵（記録者）、上記電子署名データ、および撮影データ本体から最終的なデータファイルを構成する。なお、ダイジェスト化の方法や、暗号系の計算処理については、他の文献に詳しいので省略する。ここでは、自分の公開鍵も、署名確認のための情報として同時に添付している。

【００５１】また、ここで特筆すべきなのは、これだけのセキュリティ機構を持ったカメラであっても、自分のデジタル署名を付加できるのは、撮影時だけという事である。他人からの受け取ったデータに対して暗号化されたものであろうと、デジタル署名付きであろうと、それを、この実施例で、あらためてデジタル署名をつけることは不可能になっている。従って、機器ＩＤ管理のセキュリティレベルを高くすれば、この機器のＩＤを持つ画像は、かならず、撮影された画像そのままであるということが自動的に証明される。

【００５２】ここで、機器固有ＩＤによるセキュリティ保証について図９を参照して説明する。例えば、６５５３６台の機器を管理する場合を想定する。この場合、機器固有ＩＤを１６ビット（ソース）で表し、冗長符号化で、より大きな数値、例えば３２ビットの数値の中にランダムにばらまき、３２ビットの機器固有ＩＤを生成する。従って、適当に機器固有ＩＤを設定しても、正当な機器固有ＩＤである確率は、１／６５５３６となる。本実施例では、デジタル署名のチェックと同時に機器ＩＤの正当性をチェックしているので、機器固有ＩＤを模擬することはほぼ不可能である。

【００５３】Ｃ－３．画像のデジタル署名チェック、復号化および閲覧

また、機器の動作モードが、ＰＬＡＹ（再生）モードに設定されている、またはＰＬＡＹ（再生）モードが選択された場合には、ステップＳ３２～ステップＳ４２において、撮影したデータを、セキュリティ付きファイルに関して、閲覧／操作／確認を行う処理が実行される。

【００５４】まず、ステップＳ３２で、表示ポインタで指示されるデータファイルを取り出す。次に、ステップＳ３４で、図７のデータファイルのヘッダ領域を参照し、取り出されたデータファイルの種類を判定する。本発明では、様々なセキュリティ機能があるので、それを、ステップＳ３４～ステップＳ４０の処理で行う。

【００５５】ここで、デジタル署名付きデータの場合には、ステップＳ３６に進み、図８に示すような処理によりチェックを行う。このチェックは、自分が撮影したデータファイル（撮影したものや、過去のデータをカードや、通信を通じて入手したもの）に対しても、また、メモリカードや通信を通じて外部からやってきた、他人のデータファイルに対しても同様に行われる。

【００５６】すなわち、データファイルに添付されている公開鍵を用いて電子署名データを復号化し、ダイジェスト化されたデータを取得する。また、データファイルのデータ本体からハッシュ関数等で特徴データを抽出し、ダイジェスト化されたデータを取得する。ここで、データ本体、ヘッダ、署名のいずれでも、データのどこかに改竄、編集等が加えられた場合には、上記双方のデータは一致せず、これに対して、改竄、編集等が加えられていない場合には、上記双方のデータは一致する。また、データ本体から日時情報、機器ＩＤ、撮影者ＩＤ（ＩＤ画像）および画像データをそれぞれ切り出す。

【００５７】また、本実施例のデジタル署名付きデータファイルでは、公開鍵情報が付加されているので、ステップＳ３８で、公開鍵を登録した相手に対する暗号化処理を行えるようにするために、必要に応じて、データファイルに添付されている記録者の公開鍵を図２に示す公開鍵束メモリ８－２に登録する。

【００５８】次に、ステップＳ４２でチェック結果に応じた表示を行う。ステップＳ３６でのチェック結果により、電子署名データから取得したダイジェスト化されたデータとデータ本体から取得したダイジェスト化されたデータとが一致すれば、すなわち整合性がとれていれば、付加情報として、図１２（ａ）に示すように、画像データとともに、内容証明ができていることを示すメッセージ（「署名チェックＯＫ！」）、認証内容、撮影日や、機器ＩＤ、撮影者のＩＤ画像を表示する。

【００５９】これらの付加情報は、操作により表示のＯＮ／ＯＦＦができるようになっている。仮に、故意や意図的な編集、またはフォーマット情報の偽造の場合は、図１２（ｂ）に示すような表示となる。画像データおよび付加情報は、図８に示すように、そのままの形で保存されているので、それらを表示することは可能であるが、一旦、改竄すると、デジタル署名との一致がとれないため、警告表示となる。また、ファイルとしては、整合性があっていても、有り得ない機器固有ＩＤではないか、過去に登録されたＩＤと不整合はないか（ＩＤ画像が同じで、機器固有ＩＤが異なる等）のチェックも行っており、不整合であれば、図１２（ｃ）に示すような表示となる。

【００６０】一方、ステップＳ３４におけるファイルヘッダの判定により、暗号化ファイルであることがわかると、自分宛の暗号化であれば、自分が公開した公開鍵で暗号化されているはずなので、ステップＳ４０で、図１１に示すように、自分の秘密鍵で復号化処理を行う。暗号化ファイルは、その生成については後述するが、ヘッ

ダ（識別、領域情報等）・ファイルタイプ（暗号化）、暗号データ本体（特定の相手宛）、ダミーのデータ本体（公開画像データ付加）からなる。暗号化ファイルの復号化処理では、まず、上記暗号化されたデータファイルの暗号データ本体を、自分の秘密鍵で復号化し、ヘッダ、公開鍵、電子署名、データ本体からなるデータファイルを生成する。

【００６１】ここで、復号化が成功すれば、暗号化ファイルには、基本的にデジタル署名がつけられているので、そのまま、デジタル署名チェック処理であるステップＳ３６，Ｓ３８に進む。そして、データファイルに添付された公開鍵による復号化に成功すれば、ステップＳ４２において、図１２（ｄ）に示すような付加情報をつけて表示する。

【００６２】一方、暗号化されたデータファイルが破壊されたり、途中で少しでも改竄されていた場合には、図１１に示すように、秘密鍵による復号化に失敗するので、ステップＳ３６，Ｓ３８の処理はスキップされる。そして、この場合には、図１２（ｅ）に示すような表示となる。本実施例では、図１０または図１１に示すように、暗号化ファイルの生成時に、ダミーのデータ本体部分に、警告情報や宣伝広告を示す公開画像データを埋め込むことを可能にしているので（詳細は後述）、図１２（ｅ）に示す例では、ファイルが壊れているか、自分宛ではない暗号ファイルである旨のメッセージが表示されるとともに、公開画像データが表示される。

【００６３】また、通常のセキュリティ保証のない、画像データからフォーマット変換された場合や、編集等を行うとセキュリティ情報を取り去る機能のある画像編集ツールを通った場合などの、セキュリティ情報がない画像データに対しては、直接ステップＳ４２へ進み、図１２（ｃ）に示すように、その旨、表示する。データが付加されている分には、日付情報等の付加情報が保証なしで表示される。

【００６４】Ｃ－４．画像データの暗号化等

上述したステップＳ４２において画像データを表示すると、図６に示すステップＳ４４へ進み、キー操作を判別し、判別したキー操作に応じて、格納画像に対して、暗号化その他の処理を行う。

【００６５】ここで、操作／編集キーが操作された場合には、ステップＳ４６へ進み、表示ポインタの移動や、削除、表示画像の送り、戻し操作などの編集処理を行う。なお、詳細は、通常のモニタ付きデジタル電子スチルカメラに準ずるので説明を省略する。

【００６６】また、暗号化処理に対するキー操作が行われた場合には、現在表示されている画像に対して、暗号化処理に入る。まず、暗号化するには、送付先相手の公開鍵が必要なので、ステップＳ４８で、公開鍵束メモリ８－２に格納されている、他ユーザのＩＤ画像の選択画面を表示し（図１３を参照）、その中から、画像で送付先ＩＤを選択する。なお、暗号化として自分に向けて暗号化することも可能である。この場合、メモリカードや、通信で誤って秘密の画像データを送ってしまっても、他人には復元することが不可能となる。

【００６７】選択が終了すると、公開鍵束メモリ８－２から、該ＩＤユーザの公開鍵を取り出し、ステップＳ５０で、図１０に示す暗号化処理を行う。すなわち、前述したステップＳ３０で作成したデジタル署名を付加したデータファイルを、上記送付先の相手の公開鍵で暗号化し、暗号化データを生成する。次に、ヘッダ（識別、領域情報等）、上記暗号化データ本体、ダミーのデータ本体から新たな（暗号化された）データファイルを生成する。また、必要に応じて、ダミーのデータ本に公開用画像の埋め込みなども行う。図示の例では、データの問い合わせ先の電話番号を画像データで埋め込んでいる。暗号化が終了したデータファイルは、ステップＳ５２で、新たなファイルとして画像記録用メモリ２に格納する。

【００６８】Ｃ－５．通信処理

また、図５に示すステップＳ２６において、機器の動作モードが、通信モードに設定されている、または選択された場合には、図５に示すステップＳ５４へ進み、通信部１０により、図１４に示すように、シリアルポートや内蔵モデム等を用いて、他のカメラやパソコンに対してデータファイルを送信（または受信）する。デジタル署名付きのデータファイルの経路には、例えば、インターネット（ＨＴＴＰ、ＦＴＰサーバ）２１への公開、パソコン２２，２４、電子スチルカメラ２３がある。

【００６９】パソコン２２では、電子スチルカメラ２０からのデジタル署名付きのデータファイルを復元後、画像データに対して編集、改竄が行われ、さらに、電子スチルカメラ２５やパソコン２６に送信されている。この場合、パソコン２５または電子スチルカメラ２６では、データファイルに改竄が行われているので、デジタル署名が不一致となり、画像データおよび付加情報を表示することは可能であるが、警告表示となる。また、電子スチルカメラ２３では、電子スチルカメラ２０から送信された、そのままのデータファイルを受信するので、内容が保証された画像データおよび付加情報が表示される。さらに、パソコン２４では、電子スチルカメラ２０から送信されたデータファイルに対して何も操作することなく、電子スチルカメラ２７に送信しているが、この場合、電子スチルカメラ２３と同様に内容が保証された画像データおよび付加情報が表示される。

【００７０】また、暗号化されたデジタル署名付きデータファイルの経路には、例えば、電子スチルカメラ２７、パソコン２８，２９がある。この場合、電子スチルカメラ２０では、送信しようとする相手の公開鍵を予め入手し、登録しておく必要がある。言い換えると、暗号化されたデータファイルを受信しようとするユーザは、自身の公開鍵を事前公開しておく必要がある。図示の例

では、電子スチルカメラ２７、パソコン２９がこれに相当する。

【００７１】データファイルは、電子スチルカメラ２０で送信先の公開鍵により暗号化され、相手の機器に送信される。電子スチルカメラ２７またはパソコン２９では、各々、当然、自身の公開鍵で暗号化されたデータファイルを復号化することができるので、内容が保証された画像データおよび付加情報が表示される。これに対して、パソコン２８では、自身宛でないデータファイルを復号化することができない。

【００７２】なお、本実施例の、署名チェック機能等は、そのまま、パソコン上のビューワソフトとして実現する事ができる。また、このファイルフォーマットでは、簡便な操作性のため、公開鍵をファイルに埋め込む形にしている。しかしながら、あるユーザに関する、最初の公開鍵の登録はセキュリティ上重要なので、公開鍵の交換は、ファイルに埋め込まず、必ず別経路で行うとしてもよい。また、公開鍵自体の正当性を調べるために、指紋鍵（Key Finger Print）などの方式を併用する構成にすることも有効である。

【００７３】ここで、ハードウェアの分解などによる、悪意ある情報奪取に対するセキュリティ保証について説明する。本実施形態では、セキュリティに関する情報として、図１５（ａ）に示すように、機器固有ＩＤ、ＩＤ画像、秘密鍵データ、公開鍵データを、セキュリティメモリ８－１に記憶している。仮に、ハードウェアを分解するなどして、図１５（ｂ）に示すように、秘密鍵データ、公開鍵データを不法に入手し、乱数系列の取り出し手法が分かったとしても、サムネイル化前のＩＤ画像がないので、再生成の偽造複製は不可能である。また、公開される情報からの逆計算により、秘密鍵を偽造複製することは暗号化アルゴリズムからほぼ不可能である。さらに、図１５（ｃ）に示すように、機器固有ＩＤ、ＩＤ画像を不法に入手し、秘密鍵、公開鍵を偽造したとしても、機器固有ＩＤに基づいて、公開鍵の一致、不一致をチェックするので、双方が一致しない限り完全な偽造複製は不可能である。

【００７４】第１実施例では、機器に組み込むことで、記録と同時にセキュリティ情報を付加することができ、また、機器にセキュリティコードの付与手段を組み込んであり、ユーザの容易な改変、解析がしにくい利点もある。

【００７５】また、第１実施例では、デジタル電子スチルカメラの画像記録時のセキュリティ情報付加としたが、ボイスレコーダ、スキャナ、デジタル動画撮影装置など、デジタルファイルを生成する入力機器一般に適用してもよい。

【００７６】Ｄ．第２の実施形態

上述した第１の実施形態は、当事者間の暗号化によるファイル交換や、不特定多数に対するファイル開示において、撮影時点での認証情報を付加するというものであった。これは、画像の証拠性や正当性を保つためには有効であるが、本第２の実施形態では、さらに、複製や部分使用の防止に有効な構成である。

【００７７】一方、特に著作権などの保護においては、複製や部分使用を抑止する効果があるものとして、「電子透かし」がある。電子透かしの方法には種々あるが、画像を記録した時点で、電子透かし情報を入れるというのは、デジタル署名等と同じように、実現可能である。これによる効果を、図１６に示す。図示の例では、電子スチルカメラ２０で、デジタル署名付きデータファイルの画像データに電子透かしとして「０２９３４８５７３６７」を挿入し、パソコン２２に送信する。ここで、パソコン２２において、画像データ部分を取り出し、複製や編集を施し、別ファイルを生成し、インターネットや他の機器に流したとする。そして、この流出したデータファイルを他の電子スチルカメラ２３やパソコン２４で取り込み、未承認使用の疑いをチェックする。このとき、元のデータファイルの透かし情報と取りこんだデータファイルの透かし情報とが一致すれば、不正使用であることが分かる。このように、デジタル署名付きデータファイルの画像データ部分を抜き出して、不正使用されている場合にも、それが検出できることがわかる。

【００７８】単純に電子透かしを併用する方式としては、図７に示す画像データ本体の、画像データに電子透かしを挿入済みのものを使うということであるし、動作フローでいえば、図５に示すステップＳ３０の処理の前に、「電子透かし情報挿入処理」を入れるだけである。

【００７９】また、本実施例をデジタル電子スチルカメラに応用した場合の利点として、通常の画像においては、パソコンで電子透かしを後付するために、著作権ＩＤの管理会社のようなものが必要であったが、機器に埋め込んだ、図２のセキュリティメモリ８－１の機器ＩＤ情報を用いれば、権利ＩＤチェックのシステムが容易になる。

【００８０】次に、電子透かしと公開鍵をさらに高度に併用した場合の構成を図１７および図１８に示す。図１７に示す暗号化（透かし処理、電子署名処理）においては、まず、電子署名に用いる情報である公開鍵（指紋鍵でもよい）を透かし情報として圧縮済みの画像データに入れ込む。次に、該画像データ（圧縮済み、透かし処理済み）に、日時情報、機器ＩＤ、撮影者ＩＤ（ＩＤ画像）を付加し、撮影データ本体とする。そして、該撮影データ本体をダイジェスト化されたデータに対して、秘密鍵で暗号化することにより、電子署名データを生成する。さらに、ヘッダ（識別、領域情報等）・ファイルタイプ（内容証明）、公開鍵、電子署名データおよび撮影データ本体から最終的なデータファイルを生成する。

【００８１】図１８に示す復号化においては、まず、データファイルに添付されている公開鍵を用いて電子署名

データを復号化し、ダイジェスト化されたデータを取得する。また、データファイルのデータ本体からハッシュ関数等で特徴データを抽出し、ダイジェスト化されたデータを取得し、上記復元されたダイジェスト化されたデータと比較する。ここで、データ本体、ヘッダ、署名のいずれでも、データのどこかに改竄、編集等が加えられた場合には、上記双方のデータは一致せず、これに対して、改竄、編集等が加えられていない場合には、上記双方のデータは一致する。また、データ本体の画像データから取り出した透かし情報から公開鍵を取り出し、上記データファイルに添付されている公開鍵と比較し、電子透かし内容の整合性のチェックを行う。そして、それぞれの比較結果が両方とも成立していれば、偽造、改竄のいずれもが行われていないことになる。

【００８２】このように、撮影データ本体を付加することで、電子署名のチェックと、電子透かし内容の整合性のチェックを行うことできる。この場合、偽造、改竄を行うには、公開鍵暗号を破るとともに、電子透かしの除去と再挿入のプロセスが必要になり、内容保証のセキュリティレベルをさらに向上させることが可能になる。

【００８３】

【発明の効果】請求項１記載の発明によれば、入力手段から入力したデジタルデータに対し、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、電子署名手段により、鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成し、ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、最終的な閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８４】また、請求項２記載の発明によれば、復号化手段により、閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化し、判断手段により、前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断し、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示手段に表示するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８５】また、請求項３記載の発明によれば、前記入力データ本体が暗号化される前段で、特徴データ抽出手段により、入力データ本体から特徴データを抽出し、ダイジェスト化しておき、電子署名データを生成する際には、前記電子署名手段により、前記特徴データ抽出手段によりダイジェスト化されたデータを、前記鍵生成手段により生成された秘密鍵により暗号化するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８６】また、請求項４記載の発明によれば、公開鍵および秘密鍵をデジタルデータの記録者を識別するための識別データに基づいて生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８７】また、請求項５記載の発明によれば、前記識別データを、デジタルデータの記録者が選択した任意の識別画像データとしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８８】また、請求項６記載の発明によれば、間引き手段により、識別画像データを所定のサイズに間引き、該間引かれた識別画像データを前記入力手段から入力されたデジタルデータに付加情報として添付するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００８９】また、請求項７記載の発明によれば、配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データを配信相手情報記憶手段に記憶しておき、配信先選択手段により、識別画像データを指定することで、閲覧ファイルの配信相手を選択するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００９０】また、請求項８記載の発明によれば、配信相手毎に、配信相手を特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを配信相手情報記憶手段に記憶しておき、暗号化手段により、前記電子署名生成手段により生成された電子署名データを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化し、前記閲覧ファイル生成手段により、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００９１】また、請求項９記載の発明によれば、前記公開情報を、少なくとも、公開可能な画像データとしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００９２】また、請求項１０記載の発明によれば、第２の復号化手段により、前記閲覧ファイルを自身の秘密鍵により復号化した後、前記復号化手段により、前記第

２の復号化手段により復元されたデータに添付されている公開鍵で、復元されたデータに添付されている電子署名データを復号化するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【００９３】また、請求項１１記載の発明によれば、前記第２の復号化手段による復元が失敗した場合には、前記判断手段により前記閲覧ファイルが不正に入手されたと判断し、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示手段に表示するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【００９４】また、請求項１２記載の発明によれば、前記公開情報を、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであるかを示すファイル種別情報としたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【００９５】また、請求項１３記載の発明によれば、前記電子署名手段による電子署名データの生成に先立って、電子透かし手段により、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込むようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【００９６】また、請求項１４記載の発明によれば、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【００９７】また、請求項１５記載の発明によれば、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、入力手段から入力されたデジタルデータに対し、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、電子署名手段により、鍵生成手段により生成された秘密鍵で、前記記憶手段に記憶された入力データ本体を暗号化して電子署名データを生成し、いったん、第１の閲覧ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめて閲覧ファイルを生成し、次いで、該閲覧ファイルを、暗号化手段により、配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化し、さらに、第２の閲覧ファイル生成手段により、ファイル本体の種別を示すファイル種別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データをまとめて最終的な閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【００９８】また、請求項１６記載の発明によれば、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、入力手段から入力されたデジタルデータに対し、電子透かし手段により、鍵生成手段で生成された公開鍵を電子透かし情報として入れ込み、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、次いで、電子署名手段により、鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成し、閲覧ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【図面の簡単な説明】

【図１】ＲＳＡ公開鍵暗号方式を説明するためのフローチャートである。

【図２】本発明の第１の実施態様における電子スチルカメラの構成を示すブロック図である。

【図３】不揮発性メモリ８のデータ構成を示す概念図である。

【図４】電子スチルカメラの動作を説明するためのフローチャートである。

【図５】電子スチルカメラの動作を説明するためのフローチャートである。

【図６】電子スチルカメラの動作を説明するためのフローチャートである。

【図７】電子署名付きのデータファイルの生成方法を説明するための概念図である。

【図８】電子署名付きのデータファイルの復元方法を説明するための概念図である。

【図９】機器固有ＩＤによるセキュリティ保証を説明するための概念図である。

【図１０】暗号化方法を説明するための概念図である。

【図１１】暗号化された電子署名付きのデータファイルの復元方法を説明するための概念図である。

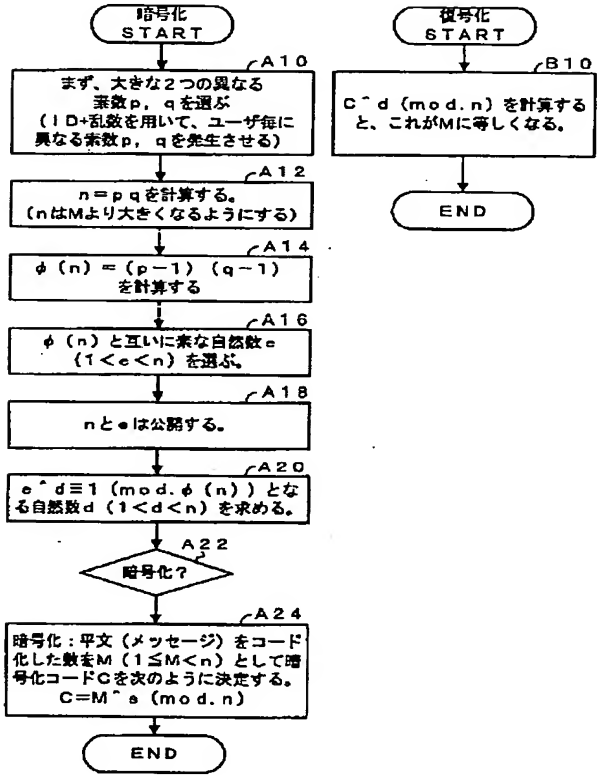
【図１２】表示例を示す概念図である。

【図１３】ＩＤ画像の例を示す概念図である。

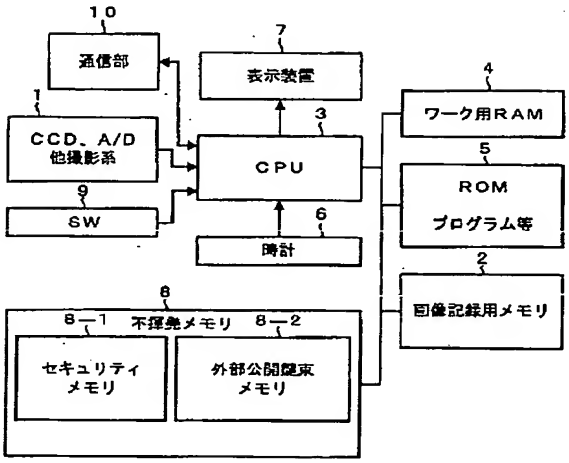
【図１４】データファイルの送信経路例を説明するための概念図である。

【図１５】情報奪取に対するセキュリティ保証を説明するための概念図である。
【図１６】本発明の第２の実施形態による電子透かしを適用した場合の概念図である。
【図１７】電子透かしを適用した場合の電子署名付きデータファイルの生成方法を説明するための概念図である。
【図１８】電子透かしを適用した場合の電子署名付きデータファイルの復元方法を説明するための概念図である。
【符号の説明】
１　撮影系
＊２　画像記録用メモリ
３　ＣＰＵ
４　ワーク用ＲＡＭ
５　ＲＯＭ
６　計時部
７　表示装置
８　不揮発メモリ
８－１　セキュリティメモリ
８－２　公開鍵束メモリ
９　スイッチ部
１０　通信部

【図１】



【図２】



【図３】

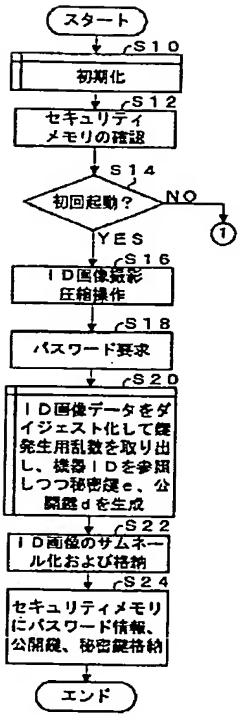
（a）

機器固有ＩＤ
ＩＤ画像サムネールデータ（16×16）等
パスワード情報
秘密鍵データ
公開鍵データ

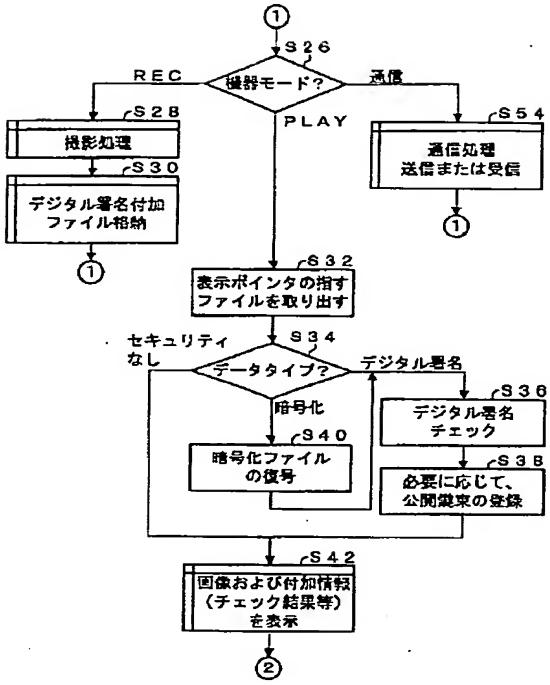
（b）

インデックス情報	
ユーザA	公開鍵
	ＩＤ画像
	機器ＩＤ
ユーザB	公開鍵
	ＩＤ画像
	機器ＩＤ

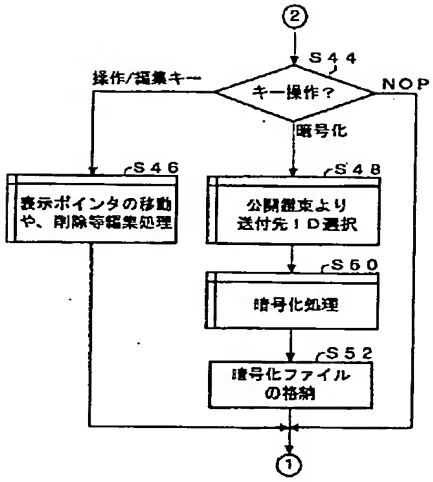
【図４】



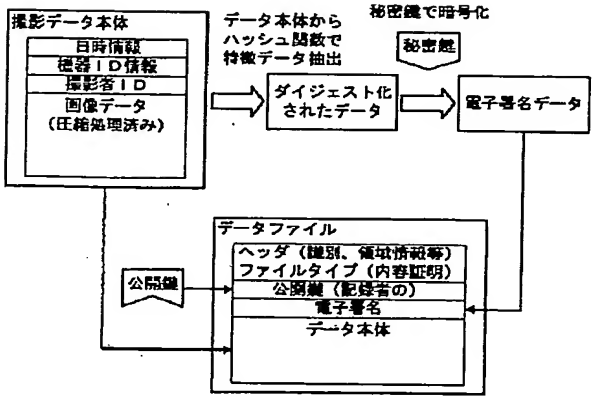
【図５】



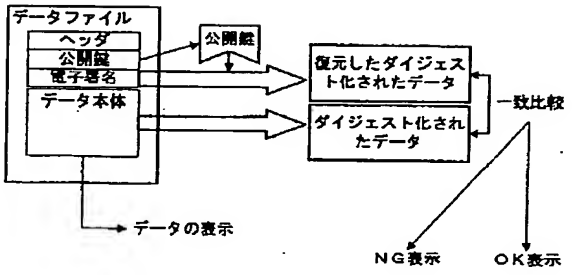
【図６】



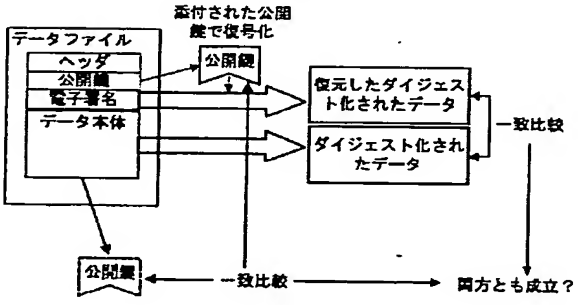
【図７】



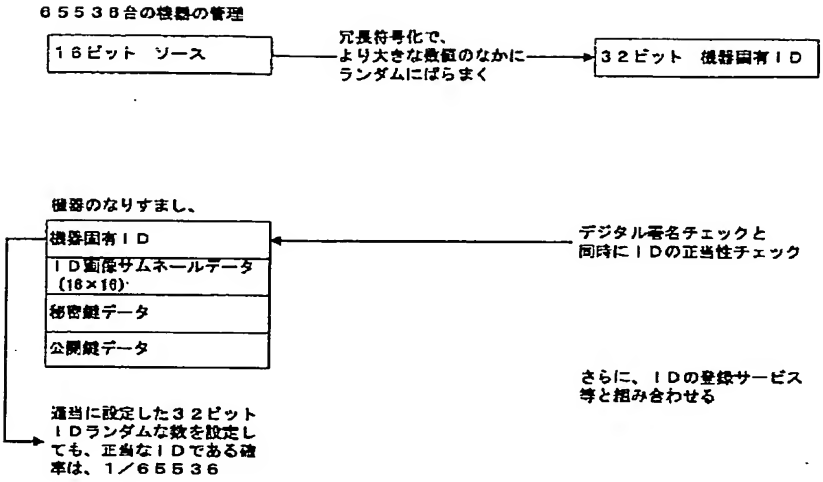
【図８】



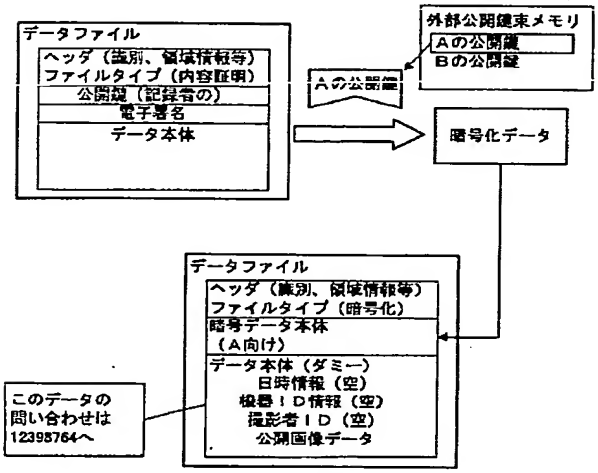
【図１８】



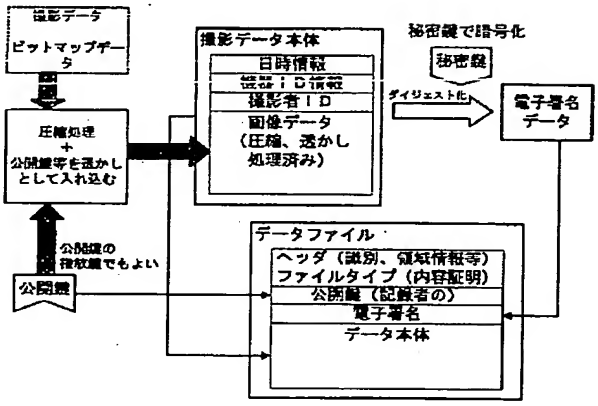
【図９】



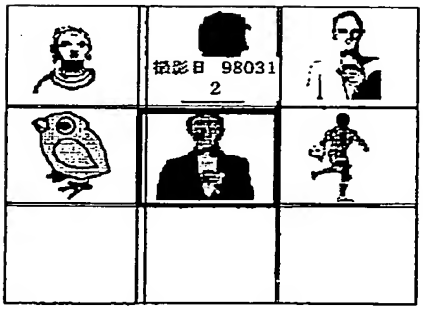
【図１０】



【図１７】

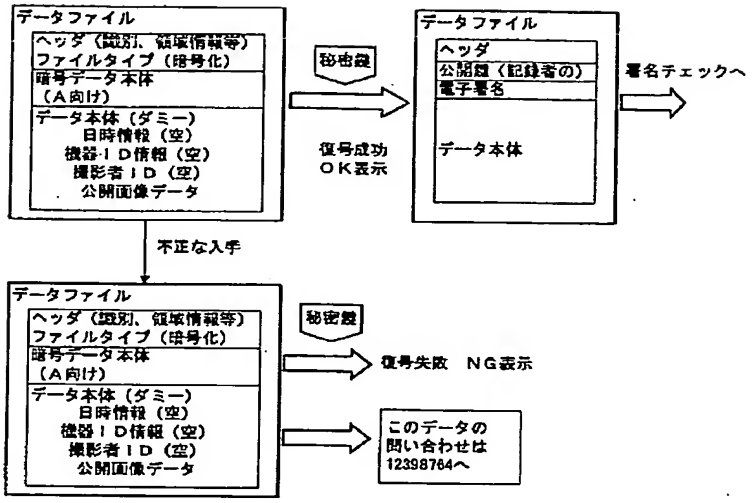


【図１３】

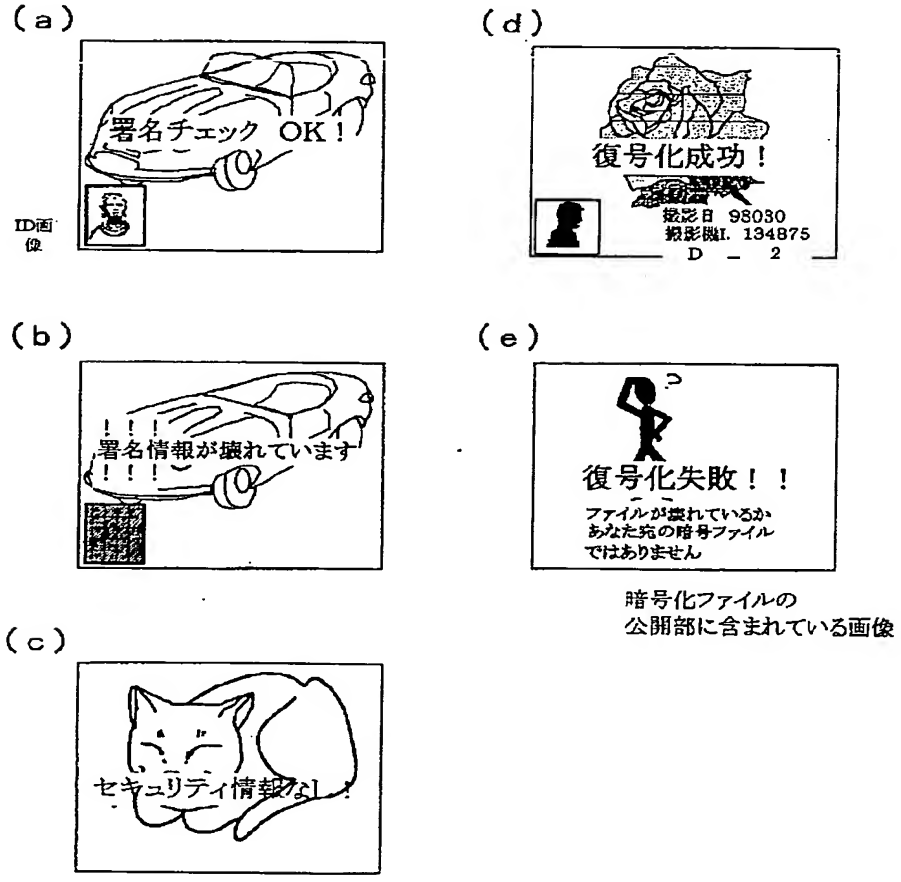


画像ID選択による
暗号化時の送付先指定

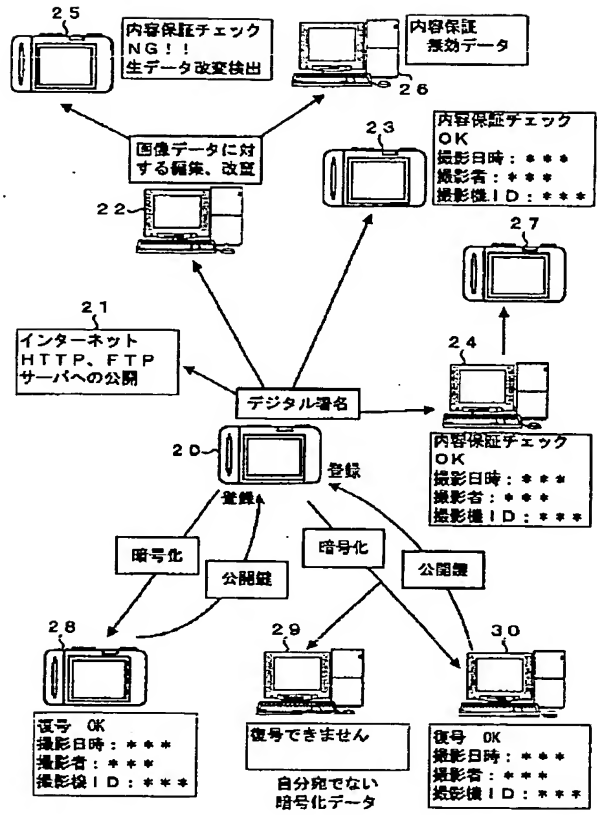
【図１１】


データファイル
ヘッダ（識別、領域情報等）
ファイルタイプ（暗号化）
暗号データ本体（A向け）
データ本体（ダミー）
日時情報（空）
機器ＩＤ情報（空）
撮影者ＩＤ（空）
公開画像データ
秘密鍵
復号成功
ＯＫ表示
データファイル
ヘッダ
公開鍵（記録者の）
電子署名
データ本体
署名チェックへ
不正な入手
データファイル
ヘッダ（識別、領域情報等）
ファイルタイプ（暗号化）
暗号データ本体（A向け）
データ本体（ダミー）
日時情報（空）
機器ＩＤ情報（空）
撮影者ＩＤ（空）
公開画像データ
秘密鍵
復号失敗　ＮＧ表示
このデータの問い合わせは12398764へ

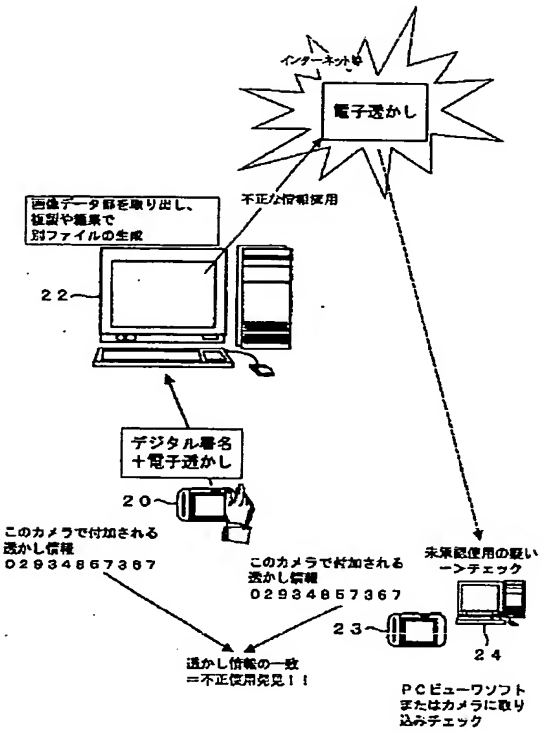
【図１２】


(a)
署名チェック　OK！
ID画像
(b)
！！！署名情報が壊れています！！！
(c)
セキュリティ情報なし！
(d)
復号化成功！
撮影日 98030
撮影機I. 134875
D － 2
(e)
復号化失敗！！
ファイルが壊れているか
あなた宛の暗号ファイル
ではありません
暗号化ファイルの
公開部に含まれている画像

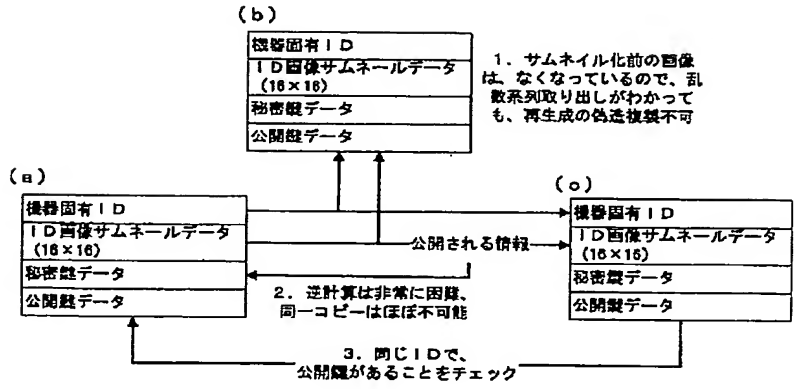
【図１４】



【図１６】



【図１５】



フロントページの続き

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｎ　1/44		Ｈ０４Ｎ　1/44	